AMENDMENT TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) In a node operative within a network of a plurality of nodes, a method for performing cryptographic-related functions, comprising:

executing an application program at the node which is not ~~physically~~ secured;

receiving an input requiring cryptographic-related processing;

generating a message via the application program based on the input, the message representing one of a predefined set of messages for processing by a cryptographic processing component located within the node;

transmitting the message to the cryptographic processing component; and

performing the cryptographic-related processing by the cryptographic processing component.

2. (previously presented) The method of claim 1, wherein the cryptographic-related processing includes at least one of:

verifying or generating a digital signature; encrypting data; decrypting data; retrieving a digital certificate or certificate revocation list; verifying a certificate's hierarchy; self-signed certificate processing; retrieving, verifying and storing a digital certificate in the node; or certificate age checking.

3. (previously presented) The method of claim 1,wherein the generating a message includes:

generating a function call message via the application program, the function call message representing a request for performing a predetermined cryptographic-related function.

4. (previously presented) The method of claim 1, further comprising:

generating an output message via the application program, the output message requiring cryptographic-related processing;

transmitting, based on the required cryptographic-related processing, one of the predefined set of messages to the cryptographic processing component;

performing the cryptographic-related processing; and

outputting the processed message.

5. (currently amended) A computer-readable medium having stored thereon a plurality of sequences of instructions that may be invoked by a plurality of predefined messages, said instructions including sequences of instructions which, when executed by a processor in an environment which is not ~~physically~~ secure, cause said processor to perform a method comprising:

receiving an input representing one of the predefined messages;

transmitting, based on the input, a function call representing a request for cryptographic-related processing to a cryptographic processing module executed by the processor; and

performing the cryptographic-related processing in the environment which is not ~~physically~~ secure.

6. (previously presented) The computer-readable medium of claim 5, wherein the performing the cryptographic-related processing includes at least one of:

verifying or generating a digital signature; encrypting or decrypting data; retrieving a digital certificate or certificate revocation list; verifying a certificate's hierarchy; self-signed certificate processing; retrieving, verifying and storing a digital certificate; or certificate age checking.

7. (canceled)

8. (original) The computer-readable medium of claim 5, wherein the input represents a digitally signed network control message requiring verification.

9. (currently amended) In an environment which is not ~~physically~~ secure, a cryptographic module, comprising:

a memory configured to operate within the environment which is not ~~physically~~ secure and to store a plurality of cryptographic processing programs on a computer-readable medium, each program being invoked via one of a plurality of predefined messages; and

a processor configured to operate within the environment and to:

receive an input requiring cryptographic-related processing,

generate one of the predefined messages based on the input,

transmit the message to the memory to invoke a first one of the cryptographic processing programs, and

perform the cryptographic-related processing.

10. (previously presented) The cryptographic module of claim 9, wherein when performing the cryptographic-related processing, the processor is configured to perform at least one of:

verifying or generating a digital signature; encrypting data; decrypting data; retrieving a digital certificate or certificate revocation list; verifying a certificate's hierarchy; self-signed certificate processing; retrieving, verifying and storing a digital certificate; or certificate age checking.

11. (original) The cryptographic module of claim 9, wherein when transmitting the message, the processor is further configured to:

transmit a function call to the first cryptographic processing program.

12. (original) The cryptographic module of claim 9, wherein the processor is further configured to:

transmit the result of the cryptographic-related processing to an application program.

13. (currently amended) In an environment which is not ~~physically~~ secure, a cryptographic module, comprising:

means, operative in the environment which is not ~~physically~~ secure, for storing a plurality of cryptographic processing programs on a computer-readable medium, each program being invoked via one of a plurality of predefined messages;

means, operative in the environment, for receiving an input requiring cryptographic-related processing;

means, operative in the environment, for generating one of the predefined messages based on the input;

means, operative in the environment, for transmitting the message to the memory to invoke a first one of the cryptographic processing programs; and

means, operative in the environment, for performing the cryptographic-related processing.

14. (currently amended) A method of performing cryptographic-related functions in a node coupled to other nodes in a network environment which is not ~~physically~~ secure, the node including an application program for handling communications with the other nodes, the method comprising:

receiving in said node within the environment which is not ~~physically~~ secure an input requiring a cryptographic-related operation;

generating in said node within the environment a predefined message based on the input, the message representing one of a plurality of predefined messages usable by a cryptographic processing program executed by the node;

transmitting in said node within the environment the predefined message to the cryptographic processing program; and

performing in said node within the environment, via the cryptographic processing program, the desired cryptographic-related operation.

15. (original) The method of claim 14, further comprising:

returning the result of the performing to the application program.

16. (previously presented) The method of claim 14, wherein the predefined message includes at least one of:

a request for digital signature generation, a request for digital signature verification, a request for data encryption, a request for data decryption, a request for retrieval of a digital certificate, a request for retrieval of a certificate revocation list, a request for verification of a certificate's hierarchy, a request for self-signed certificate processing, or a request for certificate age checking.

17. (previously presented) The method of claim 16, wherein the request for digital signature generation includes a request for at least one of RSA signature generation, secret keyed MD5 signature generation, elliptic curve signature generation or digital signature standard signature generation.

18. (previously presented) The method of claim 16, wherein the request for digital signature verification includes a request for at least one of RSA signature

verification, secret keyed MD5 signature verification, elliptic curve signature verification or digital signature standard signature verification.

19. (previously presented) The method of claim 16, wherein the request for data encryption includes a request for at least one of RSA based encryption or elliptic curve based encryption.

20. (previously presented) The method of claim 16, wherein the request for data decryption includes a request for at least one of RSA based decryption or elliptic curve based decryption.

21. (original) The method of claim 14, wherein the performing includes:

accessing a remote server via the network to retrieve cryptographic-related information.

22. (currently amended) A computer-readable medium that stores instructions executable by at least one processor in an environment which is not ~~physically~~ secure to perform a method for providing cryptographic-related functions, the method comprising:

receiving in the at least one processor in the environment which is not ~~physically~~ secure a first function call from a predefined list of function calls, the predefined list of function calls representing available cryptographic-related functions executable by the at least one processor;

generating in the at least one processor in the environment a request message based on the first function call, the request message representing a request for processing by a cryptographic processing module executed by the at least one processor;

transmitting in the at least one processor in the environment the request message to the cryptographic processing module; and

performing in the at least one processor in the environment the cryptographic-related function.

23. (canceled)